AMENDMENTS TO THE CLAIMS

The following listing of claims will replace all prior versions and listings of claims in the application.

Listing Of Claims

1. (currently amended) A security system for controlling access to a trusted computer network by a client computer, comprising:

a bastion host that controls access to said trusted computer network;

a first data store associated with said bastion host and configured to store a set of key-password pairs;

a portable storage device;

a second data store associated with said portable storage device and configured to store passwords represented in said key-password pairs;

a user operable initialization mechanism that interfaces with said first and second data stores, said initialization mechanism generating and storing said key-password pairs in said first data store and generating and storing said passwords in said second data store;

an authentication mechanism having a first component associated with said bastion host and having a second component associated with said client computer;

said first component being configured to communicate a password-specific key associated with one of said key-password pairs to said second component;

said second component being configured to access said second data store and retrieve at least one password represented in said key-password pair;

said second component being further configured to communicate said at least one password to said first component based on input from the user and based on said password-specific key communicated from said first component;

wherein said second component is further configured to prompt a user to provide an identification value, retrieve a symmetric key from a protected area within said portable storage device that is only accessible upon authentication of said portable storage device, produce an encrypted identification value by encrypting said second identification value with said symmetric key, and retrieve the password by decrypting a corresponding encrypted value in said second datastore using a combination of the encrypted identification value and the password-specific key.

2. (previously presented) The system of claim 1 further comprising a key management system that encrypts and stores said passwords in said second data store.

3. (original) The system of claim 1 wherein said passwords stored in said second data store are encrypted and said second component is configured to decrypt and communicate said at least one password to said first component.

4. (original) The system of claim 1 wherein said portable storage device is a non-volatile memory device.

5. (original) The system of claim 1 wherein said portable storage device is an optical disk.

6. (previously presented) The system of claim 1 further comprising a screening router system that blocks interaction with said trusted computer network.

7. (previously presented) The system of claim 6 further comprising a proxy system that integrates with said screening router to permit interaction with said trusted computer network under control of said authentication mechanism.

8. (previously presented) The system of claim 1 further comprising a session management system that restricts interaction with said trusted computer network to an authenticated active session.

9. (previously presented) The system of claim 1 further comprising a session management system that restricts interaction with said trusted computer network to predetermined time duration.

10. (original) The system of claim 1 further comprising a plug-in module stored on said portable storage device and accessible to said client computer to provide said client computer with instructions in implementing said second component of said authentication mechanism.

11.-16. (cancelled)

17. (withdrawn) A secure network communication system, comprising:

a screening router;

an authentication system that authenticates a remote client communicating through said screening router;

a bastion host having web proxy system in communication with said screening router;

active session middleware associated with said bastion host that associates an active session with said remote client upon authentication by said authentication system ;

said web proxy system being configured to perform URL verification and URL modification based on information received from said active session middleware and said authentication system.

18. (withdrawn) The system of claim 17 wherein said authentication system includes a portable storage device that supplies one-time passwords to said remote client.

19. (withdrawn) The system of claim 17 wherein said web proxy system performs URL modification bi-directionally and operates upon URLs issued both to and from said remote client.

20. (withdrawn) The system of claim 17 wherein said web proxy system further includes a template page database that stores at least one log-in page that integrates with said authentication system.

21. (withdrawn) The system of claim 17 wherein said authentication system is associated with a gateway and wherein said includes a secure database for storing information used by to authenticate said remote client.

22. (withdrawn) The system of claim 17 wherein said active session middleware includes session timer that terminates said active session after a predetermined time.

23. (withdrawn) The system of claim 17 wherein said authentication system employs a portable storage device having a protected area that stores a session key used during the authentication process to protect information provided by a user operating said remote client.

24. (currently amended) A security system comprising:

a gateway device situated between a trusted network and an untrusted network, which stores a set of N password-key pairs, N being an integer greater than one;

a portable storage device that stores a set of N encrypted values; and

a remote client that communicates with said gateway device via the untrusted network and accesses said portable storage device,

wherein said remote client receives a password-specific key of one of said set of password-key pairs from said gateway device, requests an identification value from a user, decrypts a corresponding encrypted value from said set of encrypted values using a combination of said identification value and said password-specific key, and transmits a result of said decryption to said gateway device, and wherein said gateway device authenticates said remote client if said result is equal to a password of said one of said set of password-key pairs;

wherein said remote client requests a first identification value from a user and sends it to said gateway device as a condition precedent to receipt of an index value and the password-specific key of one of said set of password-key pairs from said gateway device, receives the index value and the password-specific key from said gateway device, requests a second identification value from the user, retrieves a symmetric key from a protected area within said portable storage device that is only accessible upon authentication of said portable storage device, produces an encrypted identification value by encrypting said second identification value with said symmetric key, uses the index to identify a corresponding encrypted value from the set of encrypted values, and decrypts the corresponding encrypted value using a combination of the encrypted identification value and the password-specific key.

25. (previously presented) The security system of Claim 24 wherein said gateway device includes an initialization module that generates said set of password-key pairs.

26. (previously presented) The security system of Claim 24 wherein said gateway device includes an initialization module that generates said set of encrypted values.

27. (previously presented) The security system of Claim 26 wherein said initialization module requests said identification value from the user, and generates said set of encrypted values from said identification value and said set of password-key pairs.

28. (previously presented) The security system of Claim 27 wherein said initialization module generates each of said set of encrypted values by encrypting a respective password of said set of password-key pairs with a combination of a respective key of said set of password-key pairs and said identification value.

29. (previously presented) The security system of Claim 28 wherein said combination of said respective key and said identification value includes a function of said respective key and said identification value encrypted with a symmetric key.

30. (previously presented) The security system of Claim 29 wherein said function is a bitwise exclusive-or.

31. (previously presented) The security system of Claim 24 wherein said set of password-key pairs is numbered, said one of said set of password-key pairs is associated with an index number i, said gateway device sends said index number i to said remote client, and said corresponding encrypted value is selected from said set of encrypted values using said index number i.

32. (previously presented) The security system of Claim 24 wherein said gateway device filters out all packets bound for the trusted network, except for packets from said remote client once said remote client has been authenticated by said gateway device.

33. (previously presented) The security system of Claim 24 wherein said gateway device revokes authentication of said remote client after a predetermined period.

34. (previously presented) The security system of Claim 24 wherein said gateway device and said remote client communicate using a Secure Sockets Layer connection.

35. (previously presented) The security system of Claim 24 wherein said combination of said identification value and said key includes a function of said key and said identification value encrypted with a symmetric key.

36. (previously presented) The security system of Claim 35 wherein said function is a bitwise exclusive-or.

37. (previously presented) The security system of Claim 24 wherein said gateway device uses each of said set of password-key pairs at most once.

38. (previously presented) The security system of Claim 24 wherein said gateway device includes an initialization module that generates said set of password-key pairs and said set of encrypted values, and stores said set of encrypted values into said portable storage device when said portable storage device is within a perimeter of said trusted network.

39. (previously presented) The security system of Claim 24 wherein said portable storage device is associated with a user identifier, said remote client communicates said user identifier to said gateway device, and said gateway device stores a set of password-key pairs for each user identifier.

40. (currently amended) A security method comprising:

storing a set of N password-key pairs in a gateway device situated between a trusted network and an untrusted network, N being an integer greater than one;

storing a set of N encrypted values in a portable storage device;

placing the portable storage device in communication with a remote client;

communicating between the remote client and the gateway device via the untrusted network;

sending a password-specific_key of one of said set of password-key pairs to the remote client;

requesting an identification value from a user of the remote client;

creating a combination of said identification value and said password-specific key;

decrypting a corresponding encrypted value from said set of encrypted values using said combination;

transmitting a result of said decryption to the gateway device;

authenticating the remote client if said result is equal to a password of said one of said set of password-key pairs;

further comprising requesting said identification value from the user, and wherein said generating includes generating said set of encrypted values from said identification value and said set of password-key pairs.

wherein said generating includes generating each of said set of encrypted values by encrypting a respective password of said set of password-key pairs with a combination of a respective key of said set of password-key pairs and said identification value.

wherein said generating includes encrypting said identification value with a symmetric key.

further comprising storing the symmetric key in a protected area of the portable storage device that is only accessible upon authentication of the portable storage device; and

encrypting the identification value with the symmetric key stored on the portable device prior to said creating the combination, said decrypting, and said transmitting.

41. (previously presented) The method of Claim 40 further comprising generating said set of password-key pairs.

42. (previously presented) The method of Claim 40 further comprising generating said set of encrypted values;

43. (cancelled)

44. (cancelled)

45. (cancelled)

46. (previously presented) The method of Claim 45 wherein said generating includes combining said encrypted identification value with said respective key using a bitwise exclusive-or.

47. (previously presented) The method of Claim 40 further comprising: assigning each of said set of password-key pairs an index number, wherein said one of said set of password-key pairs is associated with an index number i; sending said index number i to the remote client; and selecting said corresponding encrypted value from said set of encrypted values using said index number i.

48. (previously presented) The method of Claim 40 further comprising filtering out all packets bound for the trusted network, except for packets from the remote client once the remote client has been authenticated by the gateway device.

49. (previously presented) The method of Claim 40 further comprising revoking authentication of the remote client after a predetermined period.

50. (previously presented) The method of Claim 40 further comprising establishing a Secure Sockets Layer connection between the gateway device and the remote client.

51. (previously presented) The method of Claim 40 wherein said creating includes evaluating a function of said key and said identification value encrypted with a symmetric key.

52. (previously presented) The method of Claim 51 wherein said function is a bitwise exclusive-or.

53. (previously presented) The method of Claim 40 wherein said sending uses each of said set of password-key pairs at most once.

54. (previously presented) The method of Claim 40 further comprising generating said set of password-key pairs and said set of encrypted values, and storing said set of encrypted values into the portable storage device when the portable storage device is within a perimeter of said trusted network.

55. (previously presented) The method of Claim 40 wherein the portable storage device is associated with a user identifier, and further comprising communicating said user identifier to the gateway device, and storing a set of password-key pairs in the gateway device for each user identifier.

56. (previously presented) A gateway device situated between a trusted network and an untrusted network, comprising:

a firewall module that restricts access to the trusted network;

a storage module that stores a set of N password-key pairs, N being an integer greater than one;

an initialization module that generates said set of password-key pairs, requests an identification value from a user, generates a set of N encrypted values from said set of password-key pairs and said identification value, and is capable of communicating said set of encrypted values to a portable storage device when the portable storage device is in secure communication with said gateway device; and

an authentication module that sends a password-specific key of one of said set of password-key pairs to a remote client over the untrusted network, receives a decryption result from the remote client, and authenticates the remote client if said decryption result is equal to a password of said one of said set of password-key pairs;

wherein said initialization module generates each of said set of encrypted values by encrypting a respective password of said set of password-key pairs with a combination of a respective key of said set of password-key pairs and said identification value.

wherein said combination of said respective key and said identification value includes a function of said identification value encrypted with a symmetric key and said respective key;

wherein said initialization module stores the symmetric key in a protected area of the portable storage device that is only accessible upon authentication of the portable storage device.

57. (cancelled)

58. (cancelled)

59. (previously presented) The gateway device of Claim 58 wherein said function is a bitwise exclusive-or.

60. (previously presented) The gateway device of Claim 56 wherein said set of password-key pairs is numbered, said one of said set of password-key pairs is associated with an index number i, and said authentication module sends said index number i to the remote client.

61. (previously presented) The gateway device of Claim 56 wherein said firewall module filters out all packets bound for the trusted network, except for packets from the remote client once the remote client has been authenticated.

62. (previously presented) The gateway device of Claim 56 wherein said authentication module revokes authentication of the remote client after a predetermined period.

63. (previously presented) The gateway device of Claim 56 wherein said gateway establishes a Secure Sockets Layer connection with the remote client.

64. (previously presented) The gateway device of Claim 56 wherein said authentication module uses each of said set of password-key pairs at most once.

65. (previously presented) The gateway device of Claim 56 wherein said storage module stores a plurality of sets of password-key pairs including said set of password-key pairs, each associated with a unique user identifier.

66. (previously presented) The gateway device of Claim 65 wherein said initialization module assigns a corresponding user identifier to the portable storage device.

67. (previously presented) The gateway device of Claim 56 wherein secure communication between the portable storage device and said gateway device is established by location of said portable storage device within a perimeter of said trusted network.

68. (cancelled)

69. (cancelled)

70. (cancelled)

71. (cancelled)